Technical Cybersecurity

Attack Analysis

How do you look at systems if you’re an attacker?

Attack Surface

Ways to get access to a system

- Program arguments
- Environment variables
- Configuration and data files
- External web sites or data sources
- Libraries used

Anything that goes into a running system

Attack Vectors

INDIVIDUAL ATTACKS

- An *attack surface* is a collection of *attack vectors*
  - A command line argument
  - An environment variable
  - A data file

Attack Graph

A SYSTEM HAS AN ATTACK SURFACE

- Defined by a collection of attack vectors on that system

AGGREGATE SYSTEMS ALSO HAVE ATTACK SURFACES

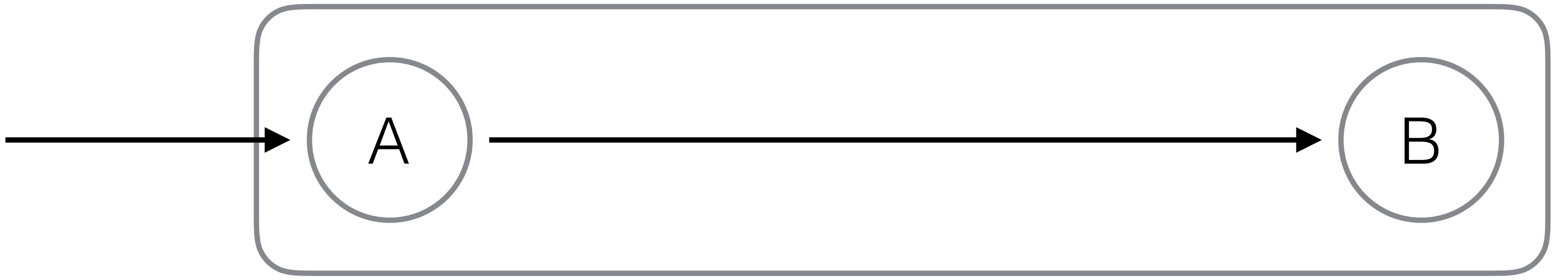
- If a system is a component in a larger system, its attack surface may be part of the larger systems attack surface
- Depends on if it’s exposed
- Depends on where the attacker is in the system

Attack graphs are a collection of *attack paths* through the larger aggregate system

Pivot

YOU *PIVOT* WHEN YOU TARGET ANOTHER SYSTEM

- In a system-of-systems, if you compromise system A, and it’s attached to system B, once you compromise A you can *pivot* and attack system B (also applies to apps on a single system)



Next up, Python!